



FortiADC - Release Notes

Version 5.3.4

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



Decemeber 11, 2019

FortiADC 5.3.4 Release Notes

TABLE OF CONTENTS

Change Log	4
Introduction	5
What's new	6
Hardware and VM support	7
Known issues	8
Resolved issues	9
Image checksums	11
Upgrade notes	12

Change Log

Date	Change Description
2019-12-11	FortiADC 5.3.4 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ Version 5.3.4, Build 0661.

To upgrade to FortiADC 5.3.4, see [FortiADC Upgrade Instructions](#).

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: <http://docs.fortinet.com/fortiadc-d-series/>.

What's new

FortiADC 5.3.4 has no new features.

Hardware and VM support

FortiADC 5.3.4 supports the following hardware models:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 100F
- FortiADC 200F
- FortiADC 300F
- FortiADC 400F
- FortiADC 1000F
- FortiADC 2000F
- FortiADC 4000F

FortiADC Release 5.3.4 supports deployment of FortiADC-VM in the following virtual machine environments:

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7
Microsoft Hyper-V	Windows Server 2012 R2
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5

Known issues

There are no known issues discovered in FortiADC 5.3.4 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Resolved issues

This section highlights the major resolved issues discovered in FortiADC 5.3.4 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Resolved issues

Bug ID	Description
0596982	Added back lbdns debug method
0596233	Did some optimization for showing the server pool status when content-routing is used
0596151	The SSL server-hello fails sometimes in some cipher combinations when working with Windows Chrome browser
0596200	Authentication Relay with "Domain Prefix Support" failed for Kerberos user principle test
0593358	Source Address (in CLI, client-address) cannot be enabled in load-balance profile
0593580	GUI can not be accessed in some circumstances
0595777	Corrected the error warning message: sftp to ftp
0571895	Corrected the incorrect port information while upgrading waf-signature
0558607	The HA config sync may fail in particular situations
0566201	Added XSS prevention in the WAF page
0536745	Vertical axis is incorrect on fortiview chart
0593281	Added memory leak prevention for vdom in some potential situations
0527984	Long name of vdom exceed frame
0588765	"VM Registration" of FortiADC selected as slave becomes "Pending" from "Valid" after establishing HA
0590421	The licd process may consume high memory in some circumstances
0516063	Optimized the SSL/TLS debug message.
0564542	No error message to block creating wad profiles that exceed maximum in different vdoms.
0579794	SIP type VS may crash in some high stress circumstances
0590120	WAF URL exception fails in some circumstances
0599700	Default value of Max Receive Window which displays under "HTTP2 Profile" tab is different from entry field value
0595611	Improve the behavior or recover time between regular RS and backup RS when the method is least-connection

Bug ID	Description
0598653	Add the long length support for TXT record
0573877	GLB CNAME record name should not the same as other records
0597406	Fixed the crash which happens in certain circumstances
0592830	Made the improvement to avoid the potential L4-VS crash in some particular conditions
0597684	DoS protection may not work in certain condition on devices that have a large amount of memory

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support contract.) In the File Name field, enter the firmware image file name including its extension, then click Get Checksum Code.

Customer Service & Support image checksum tool

The screenshot shows the Fortinet Customer Service & Support website. At the top, there is a blue header with a 'Home' link and a welcome message for 'Samuel Liu'. Below this is a 'Customer Support Bulletin' section with three items listed, each with a 'More' button. The main content area is divided into several sections: 'Asset' with 'Register/Renew' and 'Manage Products' links; 'Assistance' with 'Create a Ticket', 'Manage Tickets', 'View Active Tickets', 'Technical Web Chat', and 'Contact Support' links; 'Quick Links' with a list of links including 'Firmware Images' and 'VM Images Download' (both highlighted with a red box); and 'Resources' with a list of links including 'Customer Support Bulletin', 'Knowledge Base', 'Fortinet Video Library', 'Fortinet Document Library', 'Discussion Forums', and 'Training & Certification'.

Home | Welcome Samuel Liu
Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time.

Customer Support Bulletin

1. AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...
2. IPS engine 3.532 released to FortiGuard for FOS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FOS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...

[More](#)

Asset

[Register/Renew](#)
Register HW/Virtual appliance or software; Activate service contract or license on your registered product.

[Manage Products](#)
Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

Assistance

[Create a Ticket](#)
The recommended way to contact Fortinet support team for your registered product. Please provide detailed information in the ticket to ensure efficient support.

[Manage Tickets](#)
Check ticket status, add comment, update contact or view history etc.

[View Active Tickets](#)
Check latest active tickets for current user; update ticket information or change ticket status.

[Technical Web Chat](#)
Provide quick answers on-line for general technical questions.

[Contact Support](#)
Contact information of Fortinet worldwide support centers.

Quick Links

- [Firmware Images](#)
- [VM Images Download](#)
- [Service Updates](#)
- [Product Life Cycle](#)
- [Fortinet Service Terms & Conditions](#)
- [Guidelines, Policies & Documents](#)
- [Help Documents](#)

Resources

- [Customer Support Bulletin](#)
- [Knowledge Base](#)
- [Fortinet Video Library](#)
- [Fortinet Document Library](#)
- [Discussion Forums](#)
- [Training & Certification](#)

Upgrade notes

The backup config file in V5.2.0-5.2.4/V5.3.0-V5.3.1, which contains certificate config may not be restored properly (causing config lost). After upgrading to V5.3.2, please discard the old V5.2.x/V5.3.x config file, then backup the config file in V5.3.2 again. This should solve the problem.

Keep the old SSL version

Keep the old SSL version predefined config to allow the upgrade to continue smoothly.

TLSv1.3 handshake failure

HSM doesn't support TLSv1.3. If the HSM certificate is used in VS, the TLSv1.3 handshake will fail.

Workaround: Please uncheck the TLSv1.3 in the SSL profile if you are using the HSM certificate to avoid potential handshake failure.

Adjust boot partition

To upgrade image for VM platforms, because of the boot partition size limit before 5.1.x, please be sure to upgrade to 5.1.x image first to adjust boot partition size, then upgrade to 5.2.x and 5.3.x, or else it will report "Unmatched partition size" error when upgrading.

No such issue for physical platforms.



FORTINET®



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.